

EXHIBIT A

DONNA CURLING, an individual, et al.)
)
 Plaintiffs,)
)
 v.) CIVIL ACTION
) FILE NO.:
 BRIAN P. KEMP, in his individual capacity)
 and his official capacity as Secretary of)
 State of Georgia and Chair of the)
 STATE ELECTION BOARD, et al.,)
)
 Defendants.)

County of Fulton)
) ss.
State of Georgia)

1. I am a cybersecurity researcher based in Atlanta. I have a BS and MS in computer engineering from University of Tennessee, Knoxville. I have worked professionally in cybersecurity since 2010. I started at Oak Ridge National Lab in the Cyber and Information Security Research group. At CISR I specialized in static and symbolic analysis of binaries. I also worked with embedded systems security and conducting security assessments for the federal government. I left ORNL in 2014 and joined Bastille Networks, a local startup where I am still employed. At Bastille Networks I specialize in wireless security and applications of software defined radio.
2. On August 23, 2016 I went to 130 Peachtree Street in an attempt to meet the Fulton County election supervisor Richard Barron with the hope of gaining access to voting systems equipment so that I could conducting a wireless security

assessment as a research project. There I was told to contact Merle King at Kennesaw State University because all election equipment is managed by the Center for Election Systems at KSU.

3. On August 24, 2016 I intended to contact Merle King. Prior to doing so, I wanted to check the Center for Election Systems public website to see if there were any public documents that could give me background on CES and Merle King. I used the search “site:elections.kennesaw.edu inurl:pdf” at www.google.com and discovered what appeared to be files relating to voter registration cached by google.
4. After this discovery, I wrote a quick script to download what public files were available here: <https://elections.kennesaw.edu/sites/> , at the time a publicly accessible site. After running the script to completion I had acquired multiple gigabytes of data. This data was comprised of many different files and formats, but among them were:
 - voter registration databases filled with personally identifiable information of voters (filename *PollData.db3*)
 - Election Management System GEMs databases (.gbf and .mdb extensions)
 - PDFs of election day supervisor passwords, for example:
 - *July 2016 Primary and NP Election Runoff Password Memo.pdf*
 - Windows executables and DLLs, for example:
 - *System.Data.SQLite.DLL*
 - *ExpDbCreate.exe*
 - *ExpReport.exe*
5. Besides leaking information, the server at elections.kennesaw.edu was running a version of Drupal vulnerable to an exploit called drupageddon. Using drupageddon, an attacker can fully compromise a vulnerable server with ease. A

public advisory for drupageddon was release in 2014, alerting users that attackers would be able to execute, create, modify, and delete anything on the server.

On August 28, 2016 I sent an email to Merle King notifying him of the vulnerabilities I found.

Hello Merle,

My name is Logan Lamb, and I'm a cybersecurity researcher who is a member of Bastille Threat Research Team. We work to secure devices against new and existing wireless threats: <https://www.bastille.net/>. This past Tuesday I went to Fulton County Government Center to speak with Rick Barron about securing voting machines against wireless threats. I was then directed to contact you and the center. I'd like to collaborate with you on securing our state's election systems infrastructure against wireless attacks.

While attempting to get more background information on the center prior to contacting you, I discovered serious vulnerabilities affecting elections.kennesaw.edu.

The following google searches reveal documents that shouldn't be indexed and appear to be critical to the elections process. In addition, the Drupal install needs to be immediately upgraded from the current version, 7.31:

"site:elections.kennesaw.edu inurl:pdf"

I generally use this type of search to find documents on websites that lack search functionality. This search revealed a completely open Drupal install. Assume any document that requires authorization has already been downloaded without authorization.

"site:elections.kennesaw.edu L&A"

The second search result appears to be for disseminating critical voting system software. This is especially concerning because, as the following article states, there's a strong probability that your site is already compromised.
<https://www.drupal.org/project/drupalgeddon>
<https://www.drupal.org/SA-CORE-2014-005>

If you have any questions or concerns please contact me. I'm able to come to the center this Monday for a more thorough discussion.

Take care,
Logan

6. After having a brief conversation with Mr. King on August 29, 2016 and being assured that the issues would be remediated, I dropped the issue.

7. In late February, 2017 I told my colleague Chris Grayson about what transpired in August. He quickly confirmed the leaking of information had not been appropriately remediated. I tweaked my script and checked to see if it worked as it had in August.
8. The script was able to download the publicly available information. The data downloaded included the same data from the previous collection and new information relating to recent elections including:
 - More recent GEMs database files
 - Files relating to the presidential election, e.g.
 - *November 2016 General Election Day Password Memo.pdf*
 - *November 2016 General Voter Lookup Password Memo.pdf*
 - Very recent files, e.g. *064 (1-10-2017).pdf*
9. Given the severity and ease with which an attacker can use drupageddon, an attacker would have easily been able to gain full control of the server at elections.kennesaw.edu had they so wanted.
10. Having gained control of the server, an attacker could modify files that are downloaded by the end users of the website, potentially spreading malware to everyone who downloaded files from the website.
11. In addition to the previously mentioned files on the server, there were multiple training videos. One of these training videos instructed users to first download files from the elections.kennesaw.edu website, put those files on a memory card, and insert that card into their local county voting systems.
12. Further Affiant sayeth not.


Logan Lamb

Sworn before me this 30 day of June, 2017, in June.

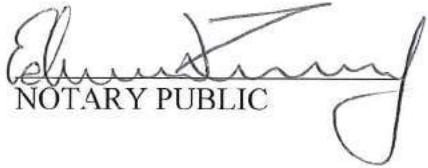

NOTARY PUBLIC



EXHIBIT B

Andino, Marci

From: Brian Newby <BNewby@eac.gov>
Sent: Tuesday, August 23, 2016 4:22 PM
To: John.Merrill@sos.Alabama.gov; stevenreed@mc-ala.org; josie.bahnke@alaska.gov; carol.thompson@alaska.gov; lealofi.uiagalelei@eo.as.gov; fiti.tavai@gmail.com; espencer@azsos.gov; rvalenzuela@risc.maricopa.gov; cpekron@ggtlaw.com; jacksoncountyclerk@gmail.com; Neal.kelley@rov.ogov.com; dwight.shellman@sos.state.co.us; rsantos@co.weld.co.us; peggy.reeves@ct.gov; tdecario@waterburyct.org; elaine.manlove@state.de.us; howard.sholl@state.de.us; Maria.Matthews@DOS.myflorida.com; flux@co.okaloosa.fl.us; bpkemp@sos.ga.gov; lbailey@augustaga.gov; maria.pangelinan@gec.guam.gov; joe.iseke@gec.guam.gov; Aulii.c.tenn@hawaii.gov; Shirley.magarifuji@mauicounty.us; thurst@sos.idaho.gov; pattyweeks@co.nezperce.id.us; bglazier@elections.il.gov; lgough@earthlink.net; bking@lec.in.gov; trethlake@co.st-joseph.in.us; carol.olson@sos.iowa.gov; gveeder@co.black-hawk.ia.us; bryan.caskey@sos.ks.gov; at_county_clerk@wan.kdor.state.ks.us; maryellen.allen@ky.gov; countyclerk@jeffersoncountyclerk.org; Angie.rogers@sos.louisiana.gov; lperret@lpclerk.com; julie.flynn@maine.gov; KLJ@portlandmaine.gov; Nikki.Charlson@Maryland.gov; katie.brown@maryland.gov; Michelle.Tassinari@sec.state.ma.us; elections@cobma.us; WilliamsS1@michigan.gov; JRoncelli@Bloomfieldtp.org; gary.poser@state.mn.us; sharon.k.anderson@co.cass.mn.us; Hawley.robertson@sos.ms.gov; bmosley@lafayettecoms.com; julie.allen@sos.mo.gov; Howell@sos.mo.gov; lkimmet@mt.gov; charlotte.mills@gallatin.mt.gov; neal.erickson@nebraska.gov; dshively@lancaster.ne.gov; jwendland@SOS.NV.gov; jpg@ClarkCountyNV.gov; astevens@sos.nh.gov; robertd@pointing.com; Robert.Giles@sos.nj.gov; lvonnessi@aol.com; Kari.Fresquez@state.nm.us; dkunko@co.chaves.nm.us; douglas.kellner@elections.ny.gov; rachel.bledi@albanycounty.com; veronica.degraffenreid@ncsbe.gov; Michael.Dickerson@mecklenburgcountync.gov; jsilrum@nd.gov; cbradley@nd.gov; pwolfe@ohiosecretaryofstate.gov; HARSMANS@mcchio.org; carol.morris@elections.ok.gov; dousan@oklahomacounty.org; james.r.williams@state.or.us; derrin.robinson@co.harney.or.us; maschneide@pa.gov; jgreenburg@mcc.co.mercer.pa.us; rallende@cee.gobierno.pr; WaValez@cee.gobierno.pr; rrock@sos.ri.gov; Andino, Marci; vr14sblack@hotmail.com; Kristin.Kellar@state.sd.us; jerry.schwartz@state.sd.us; Mark.Goins@tn.gov; astarling@tnaflcio.org; kingram@sos.texas.gov; elections@traviscountytexas.gov; mthomas@utah.gov; sswensen@slco.org; will.senning@sec.state.vt.us; dorsetclerk@gmail.com; Caroline.Fawkes@vi.gov; genevieve.whitaker@vi.gov; edgardo.cortes@elections.virginia.gov; Griddlemoser@staffordcountyva.gov; stuart.holmes@sos.wa.gov; swansonk@co.cowlitz.wa.us; lbrown@wvsos.com; bwood@putnamwv.org; michael.haas@wi.gov; bgoeckner@village.germantown.wi.us; jgonzales@co.albany.wy.us; kal.schon@wyo.gov
Cc: EAC Leadership
Subject: Attached Security Document
Attachments: BOE_FLASH_aug2016_final.pdf

Dear Standards Board Member,

On behalf of EAC Commissioner Christy McCormick, as the agency's DFO for the Standards Board, I am sending the attached security document to you that has been provided to us recently by the Federal Bureau of Investigation. The FBI has asked that we share this document expressly with election officials.

You'll see that the document identifies specific Internet Protocol (IP) addresses and recommends that election officials scan their systems to ensure these IP addresses are not accessing election systems.

Please share this with other election officials in your state, respecting the FBI's designation that this information be shared on a need-to-know basis only. The attachment is non-classified, but it is not intended for distribution outside of the election administrator community.

Should you have any questions regarding this information, please call or email me. In the meantime, thank you for your assistance regarding this information.

Brian D. Newby, CERA | Executive Director
Election Assistance Commission
1335 East West Highway | Suite 4300
Silver Spring | Maryland | 20910
(301) 563-3959 (O) | (202) 734-0639 (C)
bnewby@eac.gov | www.eac.gov



UNITED STATES
ELECTION ASSISTANCE COM.

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the system manager. The recipient is advised to check this email and any attachments for the presence of viruses. The Election Assistance Commission accepts no liability for any virus transmitted by this email.



FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

18 August 2016

Alert Number

T-LD1004-TT

WE NEED YOUR HELP!

If you find any of
these indicators on
your networks, or
have related
information, please
contact

**FBI CYWATCH
immediately.**

Email:

cywatch@ic.fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any
related information to FBI
CyWatch, you are assisting in
sharing information that
allows the FBI to track
malicious actors and
coordinate with private
industry and the United States
Government to prevent future
intrusions and attacks.*

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released TLP: AMBER: The Information in this product is only for members of their own organization and those with DIRECT NEED TO KNOW. This Information is NOT to be forwarded on beyond NEED TO KNOW recipients.

Targeting Activity Against State Board of Election Systems

Summary

The FBI received information of an additional IP address, 5.149.249.172, which was detected in the July 2016 compromise of a state's Board of Election Web site. Additionally, in August 2016 attempted intrusion activities into another state's Board of Election system identified the IP address, 185.104.9.39 used in the aforementioned compromise.

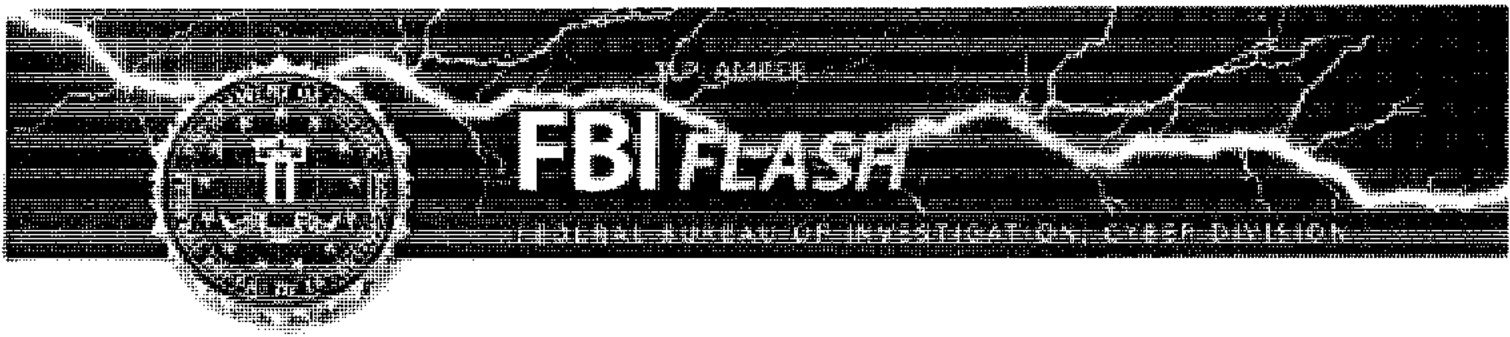
Technical Details

The following information was released by the MS-ISAC on 1 August 2016, which was derived through the course of the investigation.

In late June 2016, an unknown actor scanned a state's Board of Election website for vulnerabilities using Acunetix, and after identifying a Structured Query Language (SQL) injection (SQLi) vulnerability, used SQLmap to target the state website. The majority of the data exfiltration occurred in mid-July. There were 7 suspicious IPs and penetration testing tools Acunetix, SQLMap, and DirBuster used by the actor, detailed in the indicators section below.

Indicators associated with the Board of Elections intrusion:

- The use of Acunetix tool was confirmed when "GET /acunetix-wvs-test-for-some-inexistent-file - 443" and several requests with "wvstest=" appeared in the logs;



- The user agent for Acunetix was identified in the logs –
"Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21++(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21";
- The use of SQLMap was confirmed after "GET /status.aspx DLIDNumber=1';DROP TABLE sqlmapoutput" appeared in the logs;
- The user agent for SQLMap is "Mozilla/5.0+(Macintosh;+U;+Intel+Mac+OS+X+10.7;+en-US;+rv:1.9.2.2)+Gecko/20100316+Firefox/3.6.2 200 0 0 421" (These are easily spoofed and not inclusive of all SQLMap activity);
- The user agent for the DirBuster program is "DirBuster-1.0-RC1+(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project<http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project>)";

IP Addresses:

- 185.104.11.154
- 185.104.9.39
- 204.155.30.75
- 204.155.30.76
- 204.155.30.80
- 204.155.30.81
- 89.188.9.91
- 5.149.249.172 (new, per FBI)

Recommendations

The FBI is requesting that states contact their Board of Elections and determine if any similar activity to their logs, both inbound and outbound, has been detected. Attempts should not be made to touch or ping the IP addresses directly.

Recommended Steps for Precautions

The FBI recommends all states take the following precautions to their state Board of Election databases:

- Search logs for commands often passed during SQL injection: SELECT, INSERT, UNION, CREATE, DECLARE, CAST, EXEC, and DELETE, ', %27, –
- Search logs for privilege escalation attempts
 - Looking for references to "cmd.exe" and "xp_cmdshell" (IIS only)
 - Common to see these following SQL injection (logical next step)
 - Can limit search to entries with HTTP status code 200 (success)



- Search for signs of directory enumeration/traversal of the web server file system (used to identify the type of scripting language a web server supports)
 - Looking for series of unsuccessful connections with strange URI strings, such as:
 - GET /Login//..%5c..%5c..%5c..%5c..%5c..%5c..%5cetc/passwd
 - GET /images"OTA2NjAw%40
 - GET /Login//..../etc/passwd
 - GET /Login//..../windows/win.ini
 - Shortly after these requests you should see SQL Injection in the logs
 - May also be "..\..\."

The following recommendations were released by the MS-ISAC on 1 August 2016.

- Conduct vulnerability scans on local government and law enforcement websites and promptly remediate any vulnerabilities (or contact your hosting provider to do so on your behalf). Particular attention should be paid to SQLi vulnerabilities. Website hosting providers should also pay attention to vulnerabilities on other websites on the same server, which may provide a back-door into the local government's website.
- Ensure all software and applications, especially content management software, are fully patched.
- Create custom, general error messages for the web application to generate, as malicious cyber actors can gain valuable information, such as table and column names and data types, through default error messages generated by the database during a SQLi attack.
- Validate user input prior to forwarding it to the database. Only accept expected user input and limit input length. This can be done by implementing a whitelist for input validation, which involves defining exactly what input is authorized.
- Implement the principle of least privilege for database accounts. Administrator rights should never be assigned to application accounts and any given user should have access to only the bare minimum set of resources required to perform business tasks. Access should only be given to the specific tables an account requires to function properly.
- The database management system itself should have minimal privileges on the operating system, and since many of these systems run with root or system level access by default, it should be changed to more limited permissions.
- Isolate the web application from the SQL instructions. Place all SQL instructions required by the application in stored procedures on the database server. The use of user-created stored procedures and prepared statements (or parameterized queries) makes it nearly impossible for a user's input to modify SQL statements because they are compiled prior to adding the input. Also, have the application sanitize all user input to ensure the stored procedures are not susceptible to SQLi attacks.
- Use static queries. If dynamic queries are required, use prepared statements.



- Enable full logging on web servers and email servers to aid in forensic and legal responses if a breach does occur.

Information in this product is for official use only. No portion of this FLASH should be released to the media or the general public. Organizations should not attempt to connect to any of the IP addresses or domain names referenced in this FLASH. The indicators are being provided for network defense purposes only and any activity to these indicators or release of this material could adversely affect investigative activities.

Reporting Notice

The FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to their local FBI Field Office or the FBI's 24/7 Cyber Watch (CyWatch). Field Office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include: the date; time; location; type of activity; number of infected users; type of equipment used for the activity; name of the submitting company or organization; and a designated point of contact.

EXHIBIT C

Zimbra

mking@kennesaw.edu

Re: Vulnerability on the elections.kennesaw.edu website

From : Merle S. King <mking@kennesaw.edu>

Wed, Mar 01, 2017 11:41 PM

Subject : Re: Vulnerability on the elections.kennesaw.edu website**To :** Stephen C. Gay <sgay@kennesaw.edu>

Stephen - We will investigate and advise.

Merle

Sent from my iPad

> On Mar 1, 2017, at 11:10 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:

>

> Merle,

>

> I received the following email, and call, tonight regarding a directory traversal vulnerability on elections.kennesaw.edu. I immediately activated our Incident Response Team and, through the use of burp suite, we were able to recreate the vulnerability described below. In the vulnerability recreation, we were able to pull voter information in database files for counties across the state and the data elements included DOB, Drivers License Number, Party Affiliation, etc. Understanding the risk associated with this vulnerability, we have closed all firewall exceptions for elections.kennesaw.edu to contain the incident. I have asked Bill Moore to act as point for this incident and we need to coordinate with your team on the web logs for elections.kennesaw.edu first thing tomorrow morning. The logs will help us understand the scope of the breach and allow us to advise the CIO as to next steps.

>

> I will be temporarily out of pocket for a short time tomorrow, then remote thereafter, but your cooperation in this incident response is appreciated.

>

> Stephen C Gay CISSP CISA

> KSU Chief Information Security Officer & UITS Executive Director

> Information Security Office

> University Information Technology Services (UITS)

> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu

>

> ----- Forwarded Message -----

> From: "Andy Green" <agreen57@kennesaw.edu>
> To: "Stephen C Gay" <sgay@kennesaw.edu>
> Sent: Wednesday, March 1, 2017 9:55:27 PM
> Subject: Vulnerability on the elections.kennesaw.edu website

>

> Stephen,

>

> Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a Drupal plug-in vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for directory traversal without authentication, leaving files exposed.

>

> My friend shared with me that the exposed directories contained, among other things:

> - voter registration detail files, including DOB and full SSN.
> - PDFs of memos to county election officials which contained full credentials for ExpressPoll Election Day access, for the November 2016 election.

>

> I was able to verify the presence of the vulnerability myself, and was able to traverse directories without authenticating. I did not download any of the voter data files to verify his statement, for obvious reasons. However, I did successfully open a PDF in my browser window, located in the Fulton County Elections/ExpressPoll/ED_Files/ folder for proof of concept.

>

> The base URL of interest is <http://elections.kennesaw.edu/sites/default/files> - please note that the URL must be http, as use of https will return a 404 error.

>

> I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in

a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.

>

> If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

>

> Thanks

>

> Andy Green, MSIS

>

> Lecturer of Information Security and Assurance

> BBA-ISA program coordinator

> KSU Student ISSA chapter faculty sponsor

> KSU Offensive Security Research Club faculty sponsor

>

> Michael J. Coles College of Business

> Kennesaw State University - A Center of Academic Excellence in Information Assurance Education

> 560 Parliament Garden Way NW, MD 0405

> Kennesaw, GA 30144-5591

> agreen57@kennesaw.edu

> <http://coles.kennesaw.edu/faculty/green-andrew.php>

> Ph: 470-578-4352

> Burruss Building, Room #490

>

> 73656d7065722070617261747573

EXHIBIT D

Background

On Wednesday March 1st at 9:29pm, a member of the KSU UITS Information Security Office was contacted by a KSU faculty member regarding an alleged breach of data on the elections.kennesaw.edu server. UITS staff validated the vulnerability and notified the CIO regarding the incident. The data contained hosted on the identified server was outside the scope of student information and no student records are associated with this alleged breach. Log analysis identified that the largest file identified contained voter registration information for 6.7 million individuals.

Actions Taken

Within an hour of initial contact, the vulnerability was confirmed and firewall rules established to block access to elections.kennesaw.edu. On March 2, 2017, UITS-ISO pulled apache and Drupal logs, reported incident to USG, reset passwords, and seized the elections.kennesaw.edu server. On March 3, 2017, the FBI was engaged and the impacted server was turned over to FBI for investigation.

IT staff which were reporting within the Center for Election systems were realigned to report within the University Information Technology Services Information Security Office and a walkthrough of the area performed to validate the isolated internal network's segregation from the public network. The elections backup server – unicoi – was removed from the Center and physically secured within UITS ISO Evidence Storage.

On March 30th, KSU employees (President Olens, CIO, AVP Strategic Communications, Legal Counsel, CISO, CES Representatives) met with the FBI and US Attorney's Office regarding the outcome of the Federal Investigation. Chad Hunt shared that the investigation had yielded no data that "escalates to the point of breach". KSU Released a statement to the media on 3/31/17 as follows:

KENNESAW, Ga (Mar. 31, 2017)—Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).

University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.

"We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

Financial Impact

None, although if it was determined that the data hosted on elections.kennesaw.edu was maliciously disclosed, the notification and credit monitoring would have been approximately \$2 million.

Successes

The following list describes those actions or systems that worked as intended, or better than anticipated, during the execution of incident and breach response activities:

- The UITS ISO Incident Response process worked as intended, isolating the server and preserving evidence for later analysis and hand-off to federal authorities.
- The time between initial report and the server being isolated was approximately 60 minutes.
- The open dialog between the faculty incident reporter and the Office of the CIO staff facilitated timely notification and rapid response time.
- Having regular conversations with Legal Affairs, Strategic Communications, Center for Election Systems staff, and the Office of the CIO ensured that all parties were informed on developments, allowing for individual planning in each respective area.

Opportunities for Improvement

1. **Issue:** Poor understanding of risk posed by The Center for Election Systems IT systems. While a previous server scan and an external researcher had helped UITS understand the high threat level of CES systems, the lack of understanding the hosted data set led to an incomplete picture of the asset value. This resulted in the existence of a high risk server (High Asset Value / High Threat Level) which should have been prioritized.

Action item(s): An objective 3rd party was hired to conduct a threat assessment for externally-facing applications. In addition, funding was secured to extend the current KSU vulnerability scanning engine to allow for external scans. Once these scans are complete, a thorough analysis of all vulnerable systems will quantify the threat level and remediation plans will be developed (and incorporated into remediation projects)

Action Item Owner(s): UITS Information Security Office

2. **Issue:** Elections webserver and Unicoi backup server are running a vulnerable version of Drupal and vulnerable to exploitation.

Action Items: Elections (externally-facing) was seized immediately and Unicoi (isolated network) was seized thereafter. Both were placed in ISO Secure Storage. UITS provisioned a dedicated virtual server, FS-ES, and business documents were moved to a newly provisioned server. This share is limited the CES subnet and CES Active Directory group users. Server administrators are limited to 2 UITS ISS Staff Members.

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

3. **Issue:** CES confidential data handling processes were not defined.

Action Items: Business processes were developed, documented, and implemented to ensure confidential data is handled appropriately. CES technicians were issued IronKey encrypted hard

drives and secure FTP transfers established with Georgia Secretary of State's Office. To date, all processes have been approved by the Georgia Secretary of State's Office.

Action Item Owner: UITS-ISO, CES Staff, Georgia Secretary of State Office

4. **Issue:** Center for Election System IT staff is not aligned with the University Information Technology Services, creating a scenario in which institutional risk could be accepted without CIO awareness.

Action Items: CES IT staff reporting structure realigned to mirror UITS TSS model. CES IT staff will report directly to UITS-ISO while directly supporting the CES. Additionally, all processes will align with USG and KSU data security policies. Strategically, UITS is launching a project to engage all external IT in order to better understand university-wide IT risk.

Action Item Owner: UITS-ISO, CES Staff

5. **Issue:** Room 105a, the elections private network data closet, was not latching properly due to lock/door misalignment.

Action Items: CISO contacted Chief of Police to have lock and door aligned. Work was completed within one business day. ISO to develop processes to review access logs on a scheduled basis.

Action Item Owner: UITS-ISO, KSU UPD, CES Staff

6. **Issue:** The elections private network data closet contains a live network jack to the ~~public network~~ (Public network)

Action Items: UITS-ISO should acquire color-coded Ethernet Jack block-outs to "lock" all ports in the data closet to the public network AND to "lock" all ports to the private network outside the data closet. Key's should be maintained by ISS and ISO, necessitating consulting with UITS staff before connecting devices.

Action Item Owner: UITS-ISO, UITS-ISS

7. **Issue:** A number of IT Assets within the Center for Elections Systems have reached end-of-life and need to be replaced or migrated to different infrastructure.

1. Rackmount UPS Battery backups (one displaying warning light)

Recommendation: Replace batteries as needed and move under UITS ISS management

2. 3com Switches – Age 10+ years – No Support – L2 only

Recommendation: Replace and move under UITS ISS management

3. Dell 1950 (Windows Domain Controller) – Age 10+ years

Recommendation: Surplus

4. Dell PowerEdge R630 – Age 1 year

Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network

5. EPIC – Vision Computer – Age Unknown – Ballot creation box

Recommendation: Continue as ISO/CES managed

6. EPIC Files – Dell 1900 – Age 6+ years – Ballot backups

Recommendation: Surplus

7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS

Recommendation: Surplus

8. elections.kennesaw.edu - Age 5 years - Dell PowerEdge R610



Recommendation: Format and reinstall on CES Isolated Network as NAS

9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950

Recommendation: Surplus

10. Web server backup

Recommendation: Surplus

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

8. Issue: An operating system and application security assessment has not been conducted on the CES Isolated Network

Action Items: UITS-ISO should perform a stand-alone security assessment of the CES Isolated Network using a laptop-based scanning engine. Servers and workstations should be hardened based on the scan results and regular testing of the network scheduled.

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

9. Issue: A wireless access point was found when UITS did a walkthrough of the CES House

Action Items: Understanding the risk that a wireless access point presents to the CES isolated network, UITS-ISO should prioritize CES for wireless network upgrade and put guidelines in place which prohibit the use of non-KSU wireless devices in the house.

Action Item Owner: UITS-ISO, UITS-ISS

10. Issue: Inconsistent port colors in House 57. Data outlets throughout the building have different color bezels to indicate which network is public and which is private:

Red = analog voice/phone

Green = KSU data public network

Blue = Elections private network

White = Elections 2nd private network

Since the original cabling installation the two private networks established for elections now act as a single private network. In room 105a, the blue cables terminate to one patch panel and the white cables terminate to another patch panel. They have connected jumpers from both of these patch panels to the same switch thus eliminating any separation by the colors Blue or White.

Action Items: Jacks for the public and private network should be reinstalled to conform to campus color standards. Additionally, jacks from the public and private networks should be on different panels. The total cost of this change will be approximately \$3,000.

Action Item Owner: UITS-ISO, UITS-ISS

EXHIBIT E

From: **Michael Barnes** mbarne28@kennesaw.edu
Subject: Re: PII found on unicoi.kennesaw.edu (only open to the KSU network)
Date: March 4, 2017 at 7:11 PM
To: Merle S. King mking@kennesaw.edu
Cc: Lectra Lawhorne llawhorn@kennesaw.edu, Stephen C. Gay sgay@kennesaw.edu, sdean29@kennesaw.edu



Unicoi has been shutdown

Michael Barnes
Director
Center for Election Systems
3205 Campus Loop Road
Kennesaw State University
Kennesaw, GA 30144
ph: 470-578-6900

On Mar 4, 2017, at 6:17 PM, Merle S. King <mking@kennesaw.edu> wrote:

Working on it now

--

Merle S. King
Executive Director
Center for Election Systems
3205 Campus Loop Road; MD#5700
Kennesaw State University
Kennesaw, GA 30144
Voice: 470-578-6900
Fax: 470-578-9012

On Mar 4, 2017, at 5:51 PM, Lectra Lawhorne <llawhorn@kennesaw.edu> wrote:

Stephen,

Please call me.

Lec

On Mar 4, 2017, at 5:48 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:

Michael,

Please see below. Can you please shut this server down until we have a chance to meet on Monday to discuss the Center's needs and how best we can work together to meet them? Could you please send conformation of shutdown when completed.

Thank you,
Stephen

Sent from Nine

From: William C. Moore
Sent: Mar 4, 2017 5:44 PM
To: Stephen Gay
Cc: Chris Gaddis
Subject: Fwd: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Stephen

The Core Team is reporting that the Center if Elections server unicoi.kennesaw.edu has files containing PII. One file potentially has 5.7 records and is suspected to be files from 2010.

The server is currently only available from the campus network. We however recommend that the server be removed from the network until all PII data can be secured or removed and verified by the ISO.

Bill

William C. Moore II CISSP, MEd, MLIS

Associate Executive Director

Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg. Rm 031
1075 Canton PI
Kennesaw, GA 30144
Tel: 470-578-6620
Fax: 678-915-4940
wcmoore@kennesaw.edu

Begin forwarded message:

From: Chris Gaddis <jgaddis6@kennesaw.edu>
Date: March 4, 2017 at 17:32:24 EST
To: "William C. Moore" <wcmoore36@kennesaw.edu>
Subject: PII found on unicoi.kennesaw.edu (only open to the KSU network)

Bill,

I noticed that CES brought up Unicoi on Friday (I think its their backup server). Regardless I ran a spider tool on it and found a number of files listed since directory listing is enabled. The top file on this list has 5.7 million records of PII. The rest have a variety of different types of data and some may be completely fine to keep open to the public.

Please note that this server is ONLY open to the KSU network but even still this type of PII should not be open to the KSU network in any form without authentication.

<http://unicoi.kennesaw.edu/sites/default/files/vendors/ESandS/Primary 2010.zip> <---- main concern
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/ExpressPoll/L&AFiles/PollData.db3>
<http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/PollData.db3>
<http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/PollData.db3>
<http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/HD68 Audio.zip>
<http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/022 - Carroll.zip>
<http://unicoi.kennesaw.edu/sites/default/files/SoS Audio Proof/May 24 Primary/048 - Douglas.zip>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-10-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-100-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/001.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/ballotproof/1-275-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/1-10-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Vote Centers with Cards.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Sign Off Sheet - Ballot Proofs.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-50-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/Ballot Order.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-40-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-30-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-20-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Ballots/1-10-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/mpearso9/Proof/Audio/Sign Off Sheet - Audio Review.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/muni/Reporting Precincts with Cards.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ExpressPoll L&A/Reporting Precincts with Cards.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/Documents/Summary Statistics.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-90-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Vote Centers with Cards.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-80-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-70-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Sign Off Sheet - March 15, 2011 Proofs.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/Ballot Order.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-60-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-50-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-40-NP-FB.pdf>

<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-30-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-20-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-170-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-160-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-140-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-130-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-120-NP-FB.pdf>
<http://unicoi.kennesaw.edu/sites/default/files/ceswebadmin/Proof/Ballots/1-110-NP-FB.pdf>

Let me know if you have any questions about this.

Thanks,

Chris

Chris Gaddis SSCP
Information Security Engineer
Information Security Office
University Information Technology Services (UITS)
Kennesaw State University
Technology Services Bldg, Room 029
1075 Canton Pl, MB #3503
Kennesaw, GA 30144 USA
Phone: (470) 578-6620
Fax: (470) 578-9050
jgaddis6@kennesaw.edu